CLAIMS

Sub A2

1. A system for detecting intrusions, comprising:

an analysis engine; and

at least one sensor, configured to communicate with the analysis engine using at least one meta-protocol including a 4-tuple.

2. The system as recited in claim 1, wherein the meta-protocol includes a data packet, and the data packet includes the 4-tuple.

3. The system as recited in claim 1, wherein the 4-tuple describes a data item.

4. The system as recited in claim 3, wherein the 4-tuple comprises a semantic type, data type, data type size, and value of the data item.

5. The system as recited in claim 4, wherein the analysis engine is configured to use the data item to detect an intrusion.

6. The system as recited in claim 1, wherein the at least one sensor is configured to communicate with the analysis engine using a plurality of meta-protocols.

7. The system as recited in claim 6, wherein each of the plurality of meta-protocols includes a 4-tuple.

8. The system as recited in claim 6, wherein the analysis engine is configured to invoke the at least one sensor and specify a set of meta-protocols supported by the analysis engine, and wherein the at least one sensor is configured to select a meta-protocol from the set.

A2

9. The system as recited in claim 8, wherein the set is a null set, and the at least one sensor is configured to use a default protocol.

10. The system as recited in claim 7, wherein the analysis engine is configured to specify a set of semantic codes representing data being requested by the analysis engine.

11. The system as recited in claim 10, wherein the at least one sensor is configured to supply data associated with the semantic codes, and wherein the at least one sensor further supplies data not associated with the semantic codes.

12. The system as recited in claim 11, wherein the analysis engine is configured to disregard the data not associated with the semantic codes.

13. The system as recited in claim 10, wherein the set of semantic codes is a null set, and the at least one sensor is configured to use a default set of semantic codes.

14. The system as recited in claim 1, wherein the analysis engine is located on a first host and an instance of the at least one sensor is located on a second host apart from the first host.

15. The system as recited in claim 14, comprising a second instance of the at least one sensor, wherein the second instance is located on a host apart from the second host.

16. The system as recited in claim 1, wherein the at least one sensor includes a sensor collector in communication with the analysis engine.

17. The system as recited in claim 1, further comprising a sensor collector disposed in a communication path between the analysis engine and the at least one sensor.

18. The system as recited in claim 1, wherein the analysis engine is configured to load a rule set while the analysis engine is in operation.

19. The system as recited in claim 1, further comprising a second sensor, and wherein the analysis engine is configured to load a rule set for the second sensor while the analysis engine is in operation.

20. The system as recited in claim 19, wherein the rule set is configured to specify interactions of data from the second sensor with data from the at least one sensor.

21. The system as recited in claim 20, wherein the analysis engine is configured to ignore rules in the rule set that specify data not supplied by any sensor.

22. A method for detecting intrusions, comprising the steps of:

providing an analysis engine;

providing at least one sensor; and

defining a meta-protocol including a 4-tuple for communication between the analysis engine and the at least one sensor.

23. A computer program product for detecting intrusions on a host, the computer program product being embodied in a computer readable medium having machine readable code embodied therein for performing the steps of:

providing an analysis engine;

providing at least one sensor; and

defining a meta-protocol including a 4-tuple for communication between the analysis engine and the at least one sensor.